UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/972,371	10/05/2001	Ryuichi Iwamura	SONY-50R4813	4728

7590 02/17/2006

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/972,371	**Applicant(s)** IWAMURA, RYUICHI	
	Examiner Benjamin E. Lanier	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7 and 17-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7 and 17-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 October 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Kambiz Zand

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4/7/03

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 20 January 2006 amends claims 1, 17 and cancels claims 8-16 and 21-25. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments, filed 20 January 2006, with respect to the amended claim language have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. Claims 1, 3-5, 7, 17, 18, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781. Referring to

claim 1, Spies discloses a secure video content delivery system wherein an IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of generating a public encryption key. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). Encrypted video data is received at the set top box (Figure 7) and passed to the processor of the set top box, along with the decryption key from the IC card, to facilitate decryption of the video data (Col. 12, line 61 – Col. 13, line 10), which meets the limitation of in a digital media receiving device, accessing an encrypted signal at said first logical circuit, determining a first decryption key for said encrypted signal at said logical circuit, at said first logical circuit decrypting said encrypted signal using said first decryption key. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 3, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55), which meets the limitation of accessing a computer control program for a second portion of local of local memory at said second logical circuit. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claims 4, 5, Spies the IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of accessing said public encryption key from a first portion of local memory at said second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). The IC card functionality can be updated or changed (Col. 12, lines 1-4), which meets the limitation of replacing a computer control program stored in a second portion of local memory at said second logical circuit with a new computer control program, accessing said new computer control program from said second portion of local memory. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

Referring to claim 7, Spies discloses that the video content can be TV broadcasts (Col. 1, lines 14-29), which are transmitted in MPEG format.

Referring to claims 17, 18, 20, Spies discloses a secure video content delivery system wherein an IC card contains public/private key pairs (Figure 6 & Col. 11, lines 40-42), which meets the limitation of a second logical circuit. The IC card contains functionality to perform key management, encryption/decryption, hashing, digital signing, and authentication (Col. 11, lines 50-55). Encrypted video data is received at the set top box (Figure 7) and passed to the processor of the set top box, along with the decryption key from the IC card, to facilitate decryption of the video data (Col. 12, line 61 – Col. 13, line 10), which meets the limitation of a first logical circuit comprising a local processor and local memory. Spies does not disclose that the IC card encrypts the decryption key before the decryption key is transmitted to the set top box. Deo discloses a method of secured communication between a smart card, and a terminal that the card is inserted, wherein the communication is authenticated because data communicated from the smart card to the terminal is encrypted by the smart card using the terminal's public key so that only the terminal can decrypt the data using their own private key (Col. 7, lines 1-5). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the IC card of Spies to contain a public key of the set top box, and encrypt the decryption key using the public key of the set top box so that the encrypted decryption key can only be decrypted using the private key of the set top box in order to authenticate that the set top box is an authentic set top box as taught by Deo (Col. 2, lines 45-47).

6. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781 as applied to claim 1 above, and further in view of Schneier. Referring to claim 2, Spies does not disclose using Diffie-Hellman algorithm for key exchange. Schneier discloses using the Diffie-Hellman algorithm for public key exchange (Pages 513-514). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the Diffie-Hellman algorithm for public key exchange in the secure video content delivery system of Spies because Diffie-Hellman gets its security from the difficulty of calculating discrete logarithms in a finite field as taught by Schneier (Page 513).

7. Claims 6, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Spies, U.S. Patent No. 6,055,314, in view of Deo, U.S. Patent No. 5,721,781 as applied to claims 1, 17 above, and further in view of Yagawa, U.S. Patent No. 6,751,598. Referring to claim 6, 19, Spies and Deo do not disclose decryption routine can be updated/replaced. Yagawa discloses a digital content distribution system wherein the system provides downloadable updates of the digital content (Col. 2, lines 16-60). It would have been obvious to one of ordinary skill in the art at the

time the invention was made to upgrade/replace the decryption routine of the terminals in order to provide the user with the latest edition of programs as taught in Yagawa (Col. 4, lines 64-67).

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

Kambiz Zand
Primary AU2132